

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059357

(43)Date of publication of application : 25.02.2000

(51)Int.Cl.

H04L 9/32
G09C 1/00
H04L 9/08
H04L 12/28

(21)Application number : 10-224079

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 07.08.1998

(72)Inventor : OKA KATSUYA
CHITOKU SHINYA
SAIJO TOMOYUKI
ONO HIROYASU

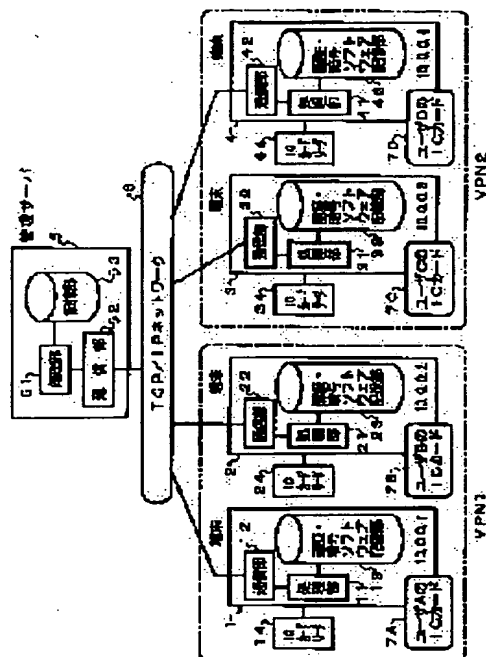
(54) CLOSED AREA GROUP COMMUNICATION SYSTEM, MANAGEMENT SERVER SYSTEM, COMMUNICATION TERMINAL AND THEIR PROGRAM STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To build up a virtual private network VPN independently of a physical condition of a network such as a terminal utilizing IP address and a work place for the user in the case of building up the virtual private network VPN on the network using the TCP/IP.

SOLUTION: User IDs and passwords of all users using a network are registered by a management server 5 and an IC card 7 (A-D) is distributed to all the users.

Furthermore, an authentication/encryption software and an IC card reader are provided to all terminals 1-4 on the network. The management server 5 configures a VPN in the unit of the user IDs and each user when using the network uses the IC card of the terminal and the user ID/password to receive the authentication by the management server 5. In this case, the management server 5 registers the IP address of the user terminal made to correspond to the VPN to which the user belongs so as to allow terminals used by users belonging to the same VPN to configure the VPN.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2000 Japanese Patent Office

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開2000-59357

(P2000-59357A)

(43)公開日 平成12年2月25日(2000.2.25)

(51)Int.Cl.	識別記号	F I	テマコード(参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D 5 J 1 0 4
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00	6 2 0 Z 5 K 0 3 3
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 D
12/28			6 7 3 A
		11/00	3 1 0 D
審査請求 未請求 請求項の数5 OL (全8頁)			

(21)出願番号 特願平10-224079

(22)出願日 平成10年8月7日(1998.8.7)

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72)発明者 岡 克也

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 千徳 真也

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74)代理人 100087848

弁理士 小笠原 吉義 (外1名)

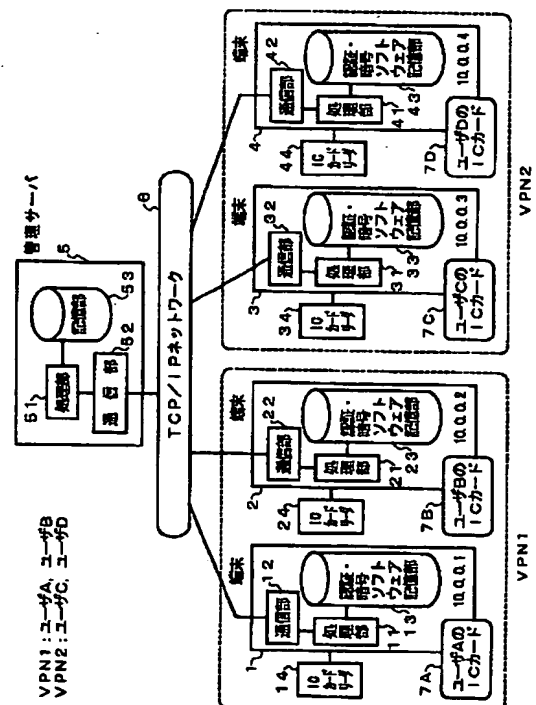
最終頁に続く

(54)【発明の名称】 閉域グループ通信システム、管理サーバ装置および通信端末、ならびにそれらのプログラム記憶媒体

(57)【要約】

【課題】TCP/IPを利用するネットワーク上で、仮想的な閉域グループ(VPN)を構築する際に、端末の利用IPアドレスや利用者の作業場所など、ネットワークの物理的条件に依存しないVPNを構築可能にする。

【解決手段】管理サーバ5に、ネットワークを利用する全ユーザのユーザIDとパスワードを登録し、全ユーザにICカード7を配布する。また、ネットワーク上の全端末1~4に、認証・暗号ソフトウェアとICカードリーダーを装備する。管理サーバ5において、ユーザIDを単位としてVPNを構成し、ユーザはネットワーク利用時に端末からICカードとユーザID・パスワードを利用して管理サーバ5にて認証を受ける。このとき、管理サーバ5がユーザ利用端末のIPアドレスをユーザの所属するVPNに対応づけて登録することにより、同一VPNに所属するユーザが利用している端末がVPNを構成する。



【特許請求の範囲】

【請求項 1】 各ユーザが持つカード型記憶媒体と、該カード型記憶媒体の入出力インタフェースを有する通信端末と、通信ネットワークを介してそれらの通信端末間の閉域グループ内での通信を行うための通信用暗号鍵を配布する管理サーバ装置から構成される閉域グループ通信システムであって、前記カード型記憶媒体は、前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵の情報を保持し、前記管理サーバ装置は、あらかじめ前記通信端末を利用する各ユーザに対して割り当てられたユーザ ID とパスワードおよび複数の閉域グループ番号と閉域グループに属するユーザ ID を管理記憶する手段と、前記通信端末から送信されてきたユーザ ID とパスワードを、該管理サーバ装置の秘密鍵を用いて復号化し、ユーザ ID とパスワードが認証できた場合には、該ユーザ ID が属する閉域グループの通信用暗号鍵を該ユーザ ID を持つユーザの公開鍵によって暗号化し、前記通信端末へ送信する手段とを備え、前記通信端末は、前記入出力インタフェースに差し込まれた前記カード型記憶媒体から、前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵を読み出す手段と、該管理サーバ装置の公開鍵を用いてユーザ ID とパスワードを暗号化し、通信ネットワークを介して前記管理サーバ装置に送信する手段と、前記管理サーバ装置から送信されてきた閉域グループ内通信端末との通信用暗号鍵を受信して前記ユーザ個々の秘密鍵により復号化する手段と、該復号化した通信用暗号鍵を用いて通信端末相互における通信情報を暗号化し、閉域グループ内通信端末相互の通信を行う手段とを備えることを特徴とする閉域グループ通信システム。

【請求項 2】 通信ネットワークを介して通信端末間の閉域グループ内での通信を行うための通信用暗号鍵を配布する管理サーバ装置であって、あらかじめ閉域グループ内での通信を行う各ユーザに対して割り当てられたユーザ ID とパスワードおよび複数の閉域グループ番号と閉域グループに属するユーザ ID を管理記憶する手段と、前記ユーザが利用する通信端末から送られてきたユーザ ID とパスワードであって、該通信端末が各ユーザにあらかじめ配布されたカード型記憶媒体から読み出した該管理サーバ装置の公開鍵を用いて暗号化したユーザ ID とパスワードを、該管理サーバ装置の秘密鍵を用いて復号化し、ユーザ ID とパスワードが認証できた場合には、該ユーザ ID が属する閉域グループの通信用暗号鍵を該ユーザ ID を持つユーザの公開鍵によって暗号化し、前記通信端末へ送信する手段とを備えることを特徴とする管理サーバ装置。

【請求項 3】 管理サーバ装置から配布された通信端末間の閉域グループ内での通信を行うための通信用暗号鍵を用いて、通信ネットワークを介して通信を行う通信端末であって、カード型記憶媒体の入出力インタフェースと、あらかじめ前記管理サーバ装置の公開鍵およびユー

ザ個々の秘密鍵の情報が格納されたカード型記憶媒体から、前記入出力インタフェースを介して前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵を読み出す手段と、該管理サーバ装置の公開鍵を用いてユーザ ID とパスワードを暗号化し、通信ネットワークを介して前記管理サーバ装置に送信する手段と、前記管理サーバ装置から送信されてきた閉域グループ内通信端末との通信用暗号鍵を受信して前記ユーザ個々の秘密鍵により復号化する手段と、該復号化した通信用暗号鍵を用いて通信端末相互における通信情報を暗号化し、閉域グループ内通信端末相互の通信を行う手段とを備えることを特徴とする通信端末。

【請求項 4】 通信ネットワークを介して通信端末間の閉域グループ内での通信を行うための通信用暗号鍵を配布する管理サーバ装置が用いるプログラムを格納したプログラム記憶媒体であって、あらかじめ閉域グループ内での通信を行う各ユーザに対して割り当てられたユーザ ID とパスワードおよび複数の閉域グループ番号と閉域グループに属するユーザ ID を管理記憶する処理と、前記通信端末から送られてきた暗号化されたユーザ ID とパスワードを、該管理サーバ装置の秘密鍵を用いて復号化する処理と、復号化されたユーザ ID とパスワードを、あらかじめ登録されたユーザ ID とパスワードとの照合により認証する処理と、ユーザ ID とパスワードが認証できた場合に、該ユーザ ID が属する閉域グループの通信用暗号鍵を該ユーザ ID を持つユーザの公開鍵によって暗号化し、前記通信端末へ送信する処理とを、計算機に実行させるプログラムを格納したことを特徴とする管理サーバ装置のプログラム記憶媒体。

【請求項 5】 管理サーバ装置から配布された通信端末間の閉域グループ内での通信を行うための通信用暗号鍵を用いて、通信ネットワークを介して通信を行う通信端末が用いるプログラムを格納したプログラム記憶媒体であって、あらかじめ前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵の情報が格納されたカード型記憶媒体から、入出力インタフェースを介して前記管理サーバ装置の公開鍵およびユーザ個々の秘密鍵を読み出す処理と、該管理サーバ装置の公開鍵を用いてユーザ ID とパスワードを暗号化し、通信ネットワークを介して前記管理サーバ装置に送信する処理と、前記管理サーバ装置から送信されてきた閉域グループ内通信端末との通信用暗号鍵を受信して前記ユーザ個々の秘密鍵により復号化する処理と、該復号化した通信用暗号鍵を用いて通信端末相互における通信情報を暗号化し、閉域グループ内通信端末相互の通信を行う処理とを、計算機に実行させるプログラムを格納したことを特徴とする通信端末のプログラム記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、TCP/IPプロ

トコルを利用して端末が相互に通信可能なネットワーク上に複数の仮想的な閉域グループ（以下、VPNという）を構築し、同一VPNに所属するユーザ間の通信のみ可能な環境を提供するVPN構築技術に係わり、特にVPNがユーザの作業場所に依存しないようにした閉域グループ通信システム、管理サーバ装置および通信端末、ならびにそれらのプログラム記憶媒体に関するものである。

【0002】

【従来の技術】TCP/IPネットワーク上でVPNを構成する場合、従来は端末が利用しているIPアドレスを単位としてVPNを構成していた。

【0003】図10は従来の第1のシステム構成例、図11は従来の第2のシステム構成例を示す。図10および図11では、端末10と端末20とが同一のVPN1に属しており、端末30と端末40とが同一のVPN2に属している。管理サーバ50は、これらのVPN情報を管理する。すなわち、それぞれの端末に固定的に割り当てられたIPアドレスと、VPN1、VPN2との対応関係を管理する。管理サーバ50と各端末とは、TCP/IPネットワーク60を介して接続される。

【0004】図10では、ユーザAとユーザBとは、同一のVPN1にあるIPアドレスの端末同士であると管理サーバ50上で認識され通信することが可能であるが、図11のようにユーザBが作業場所を移動すると、管理サーバ50上では、端末10のIPアドレスと端末40のIPアドレスとは異なったVPNにあると認識されるので、ユーザAはユーザBと通信できない。

【0005】

【発明が解決しようとする課題】従来技術では、ユーザが通常利用している端末から別の端末へ作業場所を移動した場合や、通常利用している端末を別のサブネットへ移動してIPアドレスが変わった場合には、ユーザが同一VPNでありながら異なったVPNに所属する端末と通信不能になる。もし、このようなときに通信を行いたい場合には、VPNを構成する端末のIPアドレスの設定変更を、いちいちVPNを管理する管理サーバ側で行うことが必要であった。

【0006】本発明は上記問題点の解決を図り、ネットワーク上でVPNを構築する際に、端末の利用IPアドレスやユーザの作業場所など、ネットワークの物理的条件に依存しないVPNを構築できるようにし、ユーザが作業場所を変えたり、また他の端末を利用した場合でも、IPアドレスの設定変更を行うことなく、同一VPNに所属するユーザとの間でセキュアな通信を可能とすることを目的とする。

【0007】

【課題を解決するための手段】本発明は、ユーザ全員にシステム内でユニークなユーザIDとパスワードを割り当て、管理サーバにおけるVPN構成単位を、従来の端

末のIPアドレスからユーザIDへ変更し、ユーザIDと端末のIPアドレスの変換テーブルを管理することにより、物理的なネットワークに依存しないVPNを構成可能にすることを最も主要な特徴とする。

【0008】ユーザが通信ネットワークを利用する際に、ユーザIDとパスワードを用いて管理サーバによる認証を行う。認証時に、ユーザが利用する端末のIPアドレスを管理サーバに登録することにより、以降、従来のIPアドレスを単位としたVPNの技術をそのまま用いることができる。

【0009】また、認証にユーザIDとパスワードの他に、カード型記憶媒体（例えば、ICカード）を併用することにより、安全な認証を可能とする。

【0010】

【発明の実施の形態】〔本発明の実施の形態の概要〕本システムの前提条件として、任意の構成装置を用いた単一の閉域ネットワーク上で、端末は任意のサブネットに帰属しており、TCP/IPプロトコルを利用して相互に通信可能な環境となっているものとする。ネットワーク上の全ての端末からアクセス可能な管理サーバが一台存在し、ネットワークに接続する全端末には、認証・暗号ソフトウェアとICカードリーダがインストールされているものとする。

【0011】このような前提のもとで、全ネットワーク利用者（以下、ユーザという）に対して一意に英数字等からなるユーザIDとパスワードを割り当て、管理サーバに設定する。管理サーバ上で、相互に通信可能なユーザを、ユーザIDを用いてグループ化し、単一のネットワーク上に複数の仮想的な閉域グループ（VPN）を作成する。ユーザがネットワークを利用する際に、ICカードを端末のICカードリーダに挿入し、ユーザIDおよびパスワードを利用して端末から認証を行うことにより、同一VPNに所属するユーザが利用する各端末がVPNを構成するようにする。

【0012】ユーザIDを用いたVPNを構築することにより、作業端末の移動による影響を受けることなく、同一VPNに所属するユーザとの間でセキュアな通信が可能となる。

【0013】〔利用形態〕図1は、本発明の実施の形態における第1のシステム構成例を示す。本システムでは、ユーザAとユーザBとが同一VPNに属しており、ユーザCとユーザDとが同一VPNに属している。管理サーバ5は、これらのVPN情報を記憶部53に記憶し管理する。処理部51は、管理サーバ5の処理を実行する部分、通信部52はTCP/IPネットワーク6を介して各端末1～4と通信を実行する部分である。

【0014】各端末1～4は、端末における処理を実行する処理部11～41、TCP/IPネットワーク6を介して管理サーバ5や他の端末と通信を行う通信部12～42および処理部11～41が実行する認証・暗号ソ

フトウェアを記憶する認証・暗号ソフトウェア記憶部13~43を持つ。また、各端末1~4には、各ユーザA~Dが持つICカード7A~7Dを読み取るためのICカードリーダ14~44が装備されている。

【0015】図1ではユーザAが端末1、ユーザBが端末2、ユーザCが端末3、ユーザDが端末4で作業している。このとき、端末1と端末2は通信可能であり、端末3と端末4は通信可能である。しかし、それ以外の端末間での通信はできない。

【0016】図2は、本発明の実施の形態における第2のシステム構成例を示す。図2では、図1のシステムの状態から、ユーザAが端末1から端末3へ作業場所を移動し、ユーザCが端末3から端末1へ作業場所を移動している。この場合、端末1と端末3は通信可能であり、端末2と端末4は通信可能である。しかし、端末1と端末2との間、端末3と端末4との間の通信はできない。

【0017】このように、VPNを構成する端末がユーザの移動に合わせて変化するため、ユーザは作業場所に依存せずにVPN内での通信が可能である。

【0018】[各部の働き] 図1、図2に示すシステムにおける各部の働きは、以下のとおりである。

【0019】(a) 管理サーバ5

- ・全ネットワーク利用者のユーザIDとパスワードと所属VPNの対応関係を管理する。
- ・全ネットワーク利用者のユーザIDとそれぞれのユーザの公開鍵の対応関係を管理する。
- ・端末からの要求に応じてユーザ認証を行う。
- ・認証に成功したら、ユーザが利用している端末のIPアドレスをユーザIDと対応づけて登録する。ユーザが利用している端末に対して、個々のVPN内通信に必要な通信用暗号鍵を配布する。

【0020】(b) 認証・暗号ソフトウェア記憶部13, 23, 33, 43

認証・暗号ソフトウェアは、TCP/IPネットワーク6に接続する全端末1~4に内蔵されている。ユーザIDとパスワードを暗号化し、管理サーバ5へ送信して認証を受ける。管理サーバ5から配布された通信用暗号鍵を用いて、通信パケットを暗号化し、VPN内端末間相互の通信を行う。

【0021】(c) ICカード7A~7D, ICカードリーダ14, 24, 34, 44

ネットワーク利用者毎に一枚のICカード7A~7Dを割り当てる。これらの各ICカードには暗号鍵が格納されており、ユーザは認証時にICカードを利用することによって、ユーザIDおよびパスワードの送信や、通信用暗号鍵の受信を安全に行うことができる。

【0022】[特徴・利点]

- ・本システムを利用することにより、ユーザを単位としたVPNを構成することができ、VPN内のユーザ間での通信セキュリティが確保される。

・ユーザが作業場所を移動しても、同一VPNに所属するユーザ同士の通信および通信セキュリティが確保される。

・ICカードを利用することにより、安全にユーザ認証を行うことができる。

【0023】[処理の流れ] 図3は、図1に示すシステムの実際の動作例を説明する図である。図4は、端末の処理フローチャート、図5は、管理サーバの処理フローチャートである。

【0024】実際の動作を説明するに先立ち、簡単に前提について説明する。あらかじめVPN利用ユーザは、管理サーバ5にアクセスし、ユーザID、パスワード、および利用するVPN番号を登録しておくものとする。図6は、VPN利用ユーザがあらかじめ管理サーバ5に登録したユーザIDとパスワードの例を示す。

【0025】ICカード7A~7Dには、それぞれ、管理サーバ5の公開鍵および各ユーザ毎の秘密鍵が格納されている。例えば、ユーザAのICカード7Aには、管理サーバ5の公開鍵とユーザAの秘密鍵が格納され、ユーザBのICカード7Bには、管理サーバ5の公開鍵とユーザBの秘密鍵が格納されている。端末と管理サーバ5間は公開鍵暗号化方式により暗号化・復号化を行うこととする。管理サーバ5には、管理サーバ5の秘密鍵およびユーザ毎の公開鍵が格納されている。図7は、管理サーバ5が管理するユーザ毎の公開鍵の例を示す。

【0026】ユーザAとユーザBがVPN1に所属し、ユーザCとユーザDがVPN2に所属するように設定されている。設定内容は図6に示すとおりである。各ユーザA~Dには、ユーザAのユーザIDがUSER-A、パスワードがpasswd1、同様にユーザBがUSER-B、ユーザCがUSER-C、ユーザDがUSER-Dというように、それぞれユーザIDが割り当てられている。

【0027】なお、ICカード7A~7Dの発行・管理、および管理サーバ5とユーザ毎の公開鍵・秘密鍵の発行・管理は、管理サーバ5で行う形態でもよく、また、第三者機関が発行するものを入手・使用する形態でもよい。

【0028】以下、図3に示す(1)~(26)に従って、図1に示すシステムの動作を説明する。

(1) ユーザAは、同じVPN内の他のユーザと通信を行いたい場合、端末1のICカードリーダ14へICカード7Aを挿入する。

(2) ICカードリーダ14により、ICカード7Aから管理サーバ5の公開鍵とユーザAの秘密鍵を、端末1のメモリ上へ読み出す(図4のステップS1)。

(3) 端末1は、ユーザAからユーザIDとパスワードを入力する(図4のS2)。

(4) 入力されたユーザIDとパスワードを、管理サーバ5の公開鍵で暗号化する(図4のS3)。

(5) 端末1は、管理サーバ5へ暗号化されたユーザIDとパスワードおよび端末1のIPアドレスを読み出して送信する(図4のS4)。

(6) 管理サーバ5は、端末1からの認証バケット(暗号化されたユーザIDとパスワード)を受け取り(図5のS21)、管理サーバ5の秘密鍵でユーザIDとパスワードを復号化する(図5のS22)。

(7) 次に、管理サーバ5は、ユーザIDとパスワードを図6に示す登録内容と比較して認証を行う(図5のS23)。

(8) 管理サーバ5は、この認証に成功すると、ユーザAの所属しているVPNを調べ、ユーザAから送られてきた認証バケット中のソースIPアドレス10.0.0.1を、図6に示すテーブルのIPアドレス欄にVPN1と対応づけて登録する(図5のS24)。なお、端末1から管理サーバ5へ送信する認証バケット中にIPアドレスが通信ソフトウェアにより自動設定されない場合には、端末1のIPアドレスを読み出して管理サーバ5へ送信する形でもよい。

(9) 管理サーバ5は、端末1がVPN1内で通信するために必要な通信用暗号鍵をユーザAの公開鍵で暗号化する(図5のS25)。この際、あらかじめ登録しているユーザID毎の公開鍵管理テーブル(図7)のデータを使用する。

(10) 管理サーバ5は、暗号化されたVPN1の通信用暗号鍵を端末1へ送信する(図5のS26)。

(11) 端末1は、暗号化されたVPN1の通信用暗号鍵を管理サーバ5から受信し(図4のS5)、ユーザAの秘密鍵で復号化する(図4のS6)。

(12) 端末1は、管理サーバ5に対して通信用暗号鍵の受信応答を返す(図4のS7)。

(13)~(24) 端末2で、ユーザBがICカード7BをICカードリーダー24に挿入することにより、ユーザBに対する認証処理が同様に行われ、端末2にVPN1の通信用暗号鍵が配布される。

(25)~(26) 以上の処理により、端末1と端末2は、同じ通信用暗号鍵を持つVPN1を構成するので、以後、端末1と端末2間の通信は、VPN1の通信用暗号鍵を用いたデータ暗号化によって行う(図4のS9)。なお、VPN内の通信を行うユーザ同士のIPアドレスは、管理サーバ5にアクセスして入手することにより、端末1と端末2間の通信を行うことが可能である。

【0029】ユーザCとユーザDに関しても、同様の処理を行うことにより、VPN2が構成される。ユーザA、ユーザB、ユーザC、ユーザDがそれぞれ認証を受けた後の管理サーバ5が管理する構成情報は、図8のように変化する。

【0030】図1に示すシステム構成の状態から図2に示すシステム構成の状態に変化する場合には、以下の動作となる。図9は、ユーザAとユーザCが端末1、端末

3での作業を中止する時の動作について説明した図である。以下、図9に示す(1)~(12)に従って、その動作を説明する。

(1) ユーザAは、端末1のICカードリーダー14からICカード7Aを抜き取る。端末1は、このICカード7Aの抜き取りを検出する(図4のS11)。

(2) これにより、端末1に対して、メモリ上に格納されている管理サーバ5の公開鍵とユーザAの秘密鍵の削除要求が発生する。

10 (3) 端末1は、メモリ上から管理サーバ5の公開鍵とユーザAの秘密鍵を削除する(図4のS12)。

(4) 端末1は、管理サーバ5に対してユーザAのIPアドレスクリア要求を送信する(図4のS13)。

(5) 管理サーバ5は、端末1からのユーザAのIPアドレスクリア要求を受信し(図5のS31)、ユーザAのIPアドレスをクリアする(図5のS32)。

(6) 管理サーバ5は、端末1へIPアドレスクリア応答を返す(図5のS33)。

(7)~(12) ユーザCについても同様の処理を行う。

20 【0031】以上により、端末1と端末3は、ユーザAとユーザCが認証を受ける前の状態に戻り、VPNの構成メンバーではなくなる。続いて、ユーザAは端末3で認証を受け、ユーザCは端末1で認証を受ける。このとき、端末2と端末3がVPN1を構成し、端末1と端末4がVPN2を構成する。これによって、ユーザAとユーザB、ユーザCとユーザDはそれぞれのVPN内で通信可能となる。

【0032】なお、以上の説明では、カード型記憶媒体としてICカードを用いた例を説明したが、記憶媒体であれば磁気カードや光磁気記録カードその他の記憶媒体であっても実施可能である。また、端末は固定的なものである必要はなく、カード型記憶媒体リーダー/ライターが内蔵された携帯型のものであってもよく、通信ネットワークは有線/無線いずれの形態でも本発明は実施可能である。

【0033】以上の各処理を、管理サーバ5および端末1~4のそれぞれの計算機によって実現するためのプログラムは、計算機が読み取り可能な可搬媒体メモリ、半導体メモリ、ハードディスクなどの適当な記憶媒体に格納することができる。

【0034】

【発明の効果】以上説明したように、本発明によれば、ユーザを単位とした、IPアドレスに依存しないVPNが構成できる。したがって、利用者は作業場所に依存せず、同一VPNに所属するユーザ間で通信セキュリティが確保された通信が可能である。

【図面の簡単な説明】

【図1】本発明の実施の形態における第1のシステム構成例を示す図である。

50 【図2】本発明の実施の形態における第2のシステム構

成例を示す図である。

【図3】図1に示すシステムの実際の動作例を説明する図である。

【図4】端末の処理フローチャートである。

【図5】管理サーバの処理フローチャートである。

【図6】VPN利用ユーザが管理サーバに登録したユーザIDとパスワードの例を示す図である。

【図7】管理サーバが管理するユーザ毎の公開鍵の例を示す図である。

【図8】管理サーバが管理するVPN構成情報の例を示す図である。

【図9】ユーザが端末での作業を中止する時の動作説明図である。

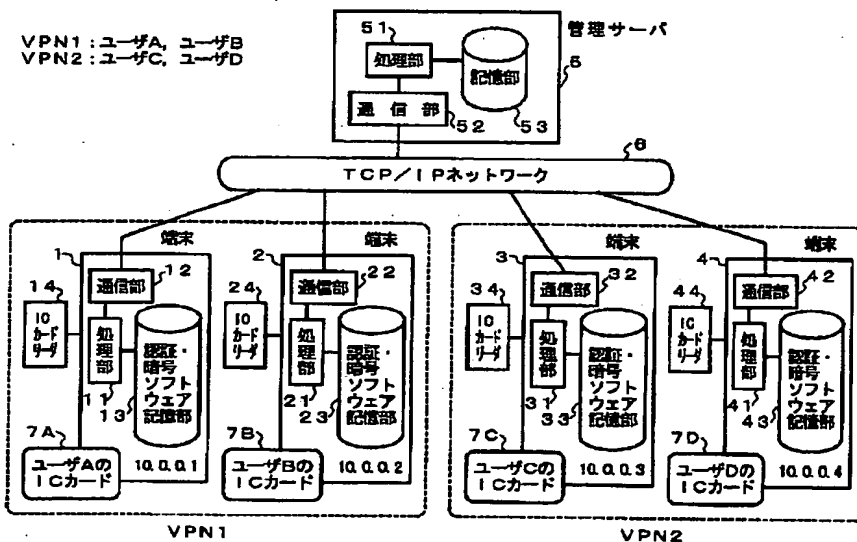
【図10】従来の第1のシステム構成例を示す図である。

【図11】従来の第2のシステム構成例を示す図である。

【符号の説明】

- 1, 2, 3, 4 端末
 11, 21, 31, 41 処理部
 12, 22, 32, 42 通信部
 13, 23, 33, 43 認証・暗号ソフトウェア記憶部
 14, 24, 34, 44 ICカードリーダー
 5 管理サーバ
 51 処理部
 52 通信部
 53 記憶部
 6 TCP/IPネットワーク
 7A, 7B, 7C, 7D ICカード

【図1】



【図6】

VPN1		
ユーザID	パスワード	IPアドレス
USER-A	passwd1	-
USER-B	passwd2	-

VPN2		
ユーザID	パスワード	IPアドレス
USER-C	passwd3	-
USER-D	passwd4	-

【図7】

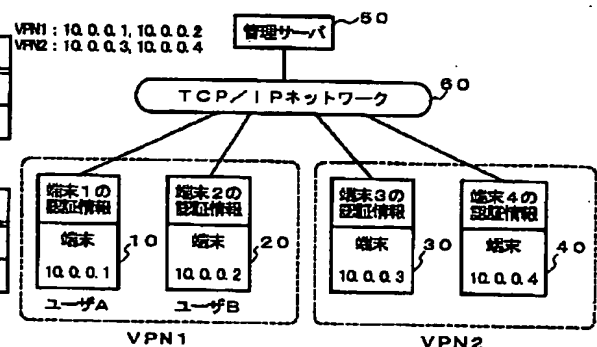
ユーザID	公開鍵
USER-A	56978
USER-B	ab379
USER-C	xy115
⋮	⋮

【図8】

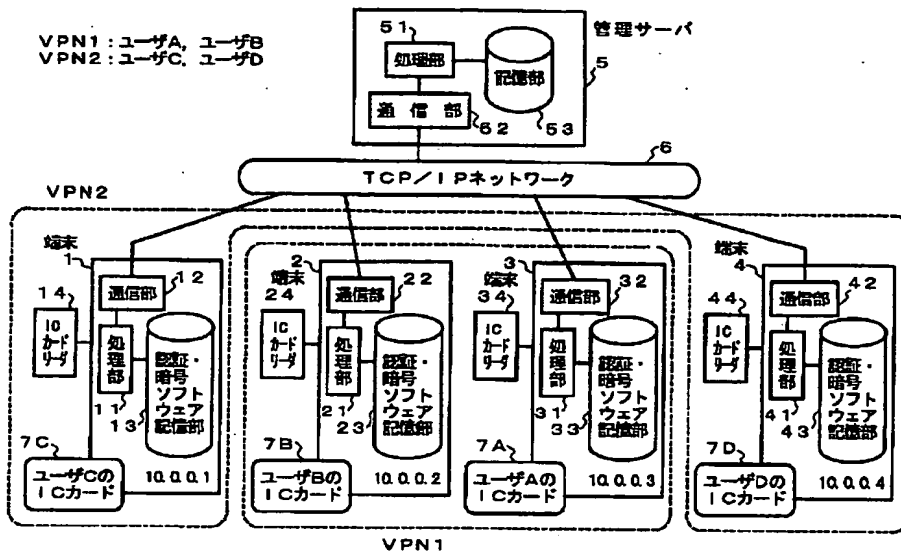
VPN1		
ユーザID	パスワード	IPアドレス
USER-A	passwd1	10.0.0.1
USER-B	passwd2	10.0.0.2

VPN2		
ユーザID	パスワード	IPアドレス
USER-C	passwd3	10.0.0.3
USER-D	passwd4	10.0.0.4

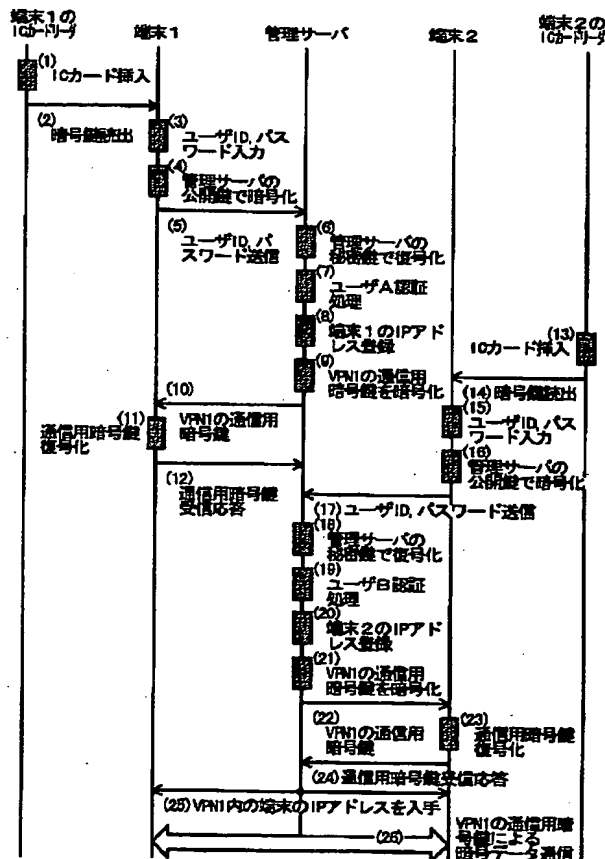
【図10】



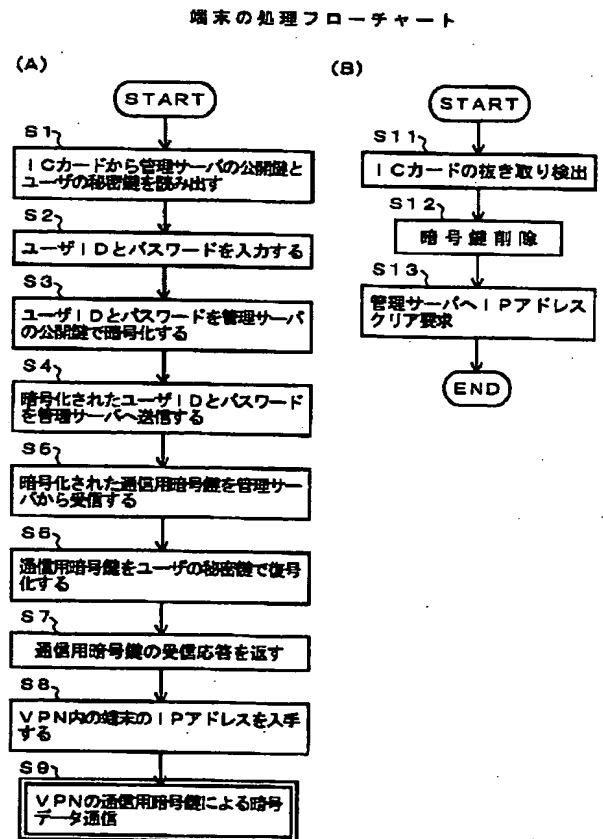
【図2】



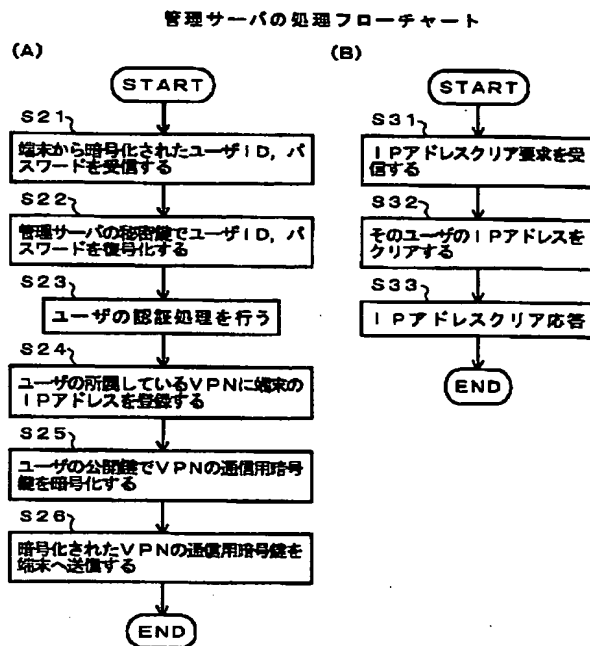
【図3】



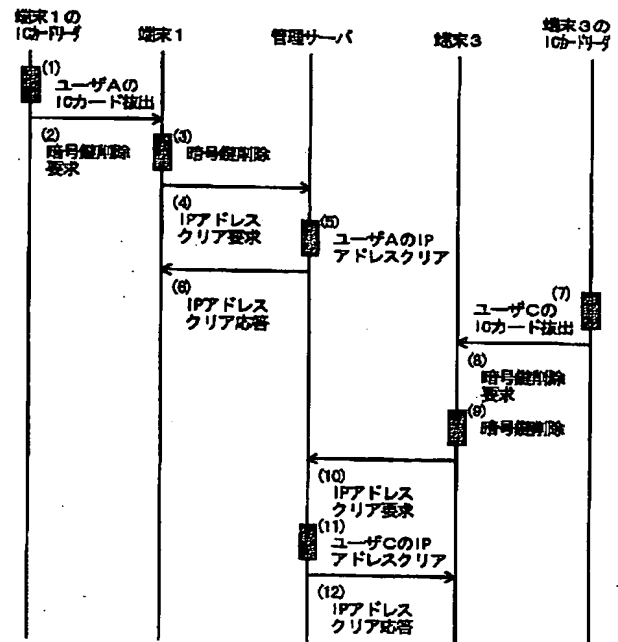
【図4】



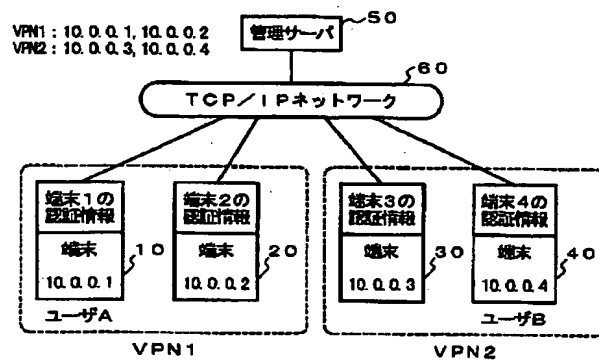
【図5】



【図9】



【図11】



フロントページの続き

(72)発明者 西條 智幸
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 小野 大泰
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

Fターム(参考) 5J104 AA07 AA16 EA19 KA02 MA01
NA02 NA05 NA06 NA33 NA37
PA07
5K033 AA08 CB01 DA01 DB10 DB12
DB14 EC03